#6
E07 (2)
& AMDT A
YN- 99
10.29.99

PATENT

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Services as First Class Mail to: Commissioner of Patents and Trademarks, Washington, DC 20231 on October 14, 1999.

Signed ______________
Mia Mitchell-Haynes

In the United States Patent and Trademark Office

Applicant: AZIZ et al.

Applicant's Ref: SUN1P342R

Serial No: 09/136,954

Filed: August 19, 1998

Title: SYSTEM FOR SIGNATURELESS TRANSMISSION AND RECEPTION OF DATA PACKETS BETWEEN COMPUTER NETWORKS

Examiner: LAUFER, P.

Group Art Unit: 2766

AMENDMENT A

Commissioner of Patents and Trademarks
Washington, D.C. 20231

Dear Sir:

In response to the Office Action dated May 18, 1999, please amend the above-identified patent application as follows:

IN THE CLAIMS:

Please **AMEND** the claims as follows:

1. (Once Amended) A method for transmitting and receiving packets of data via [a] an internetwork for a first host computer on a first computer network to a second host computer on a second computer network, the first and second computer networks including, respectively, first and second bridge computers, each of said first and second host computers and first and second bridge computers including a processor and a memory for storing instructions for execution by the processor, each of said first and second bridge computers further including memory for storing at least one predetermined encryption/decryption mechanism and information identifying a predetermined plurality of host computers as hosts requiring security for packets transmitted between them, the method being carried out [be] by means of the instructions stored on said respective memories and including the steps of:

(1) generating, by the first host computer, a first data packet for transmission to the second host computer, a portion of the first data packet including information representing an internetwork address of the first host computer and internetwork address of the second host computer;

(2) in the first bridge computer, intercepting the first data packet and determining whether the first and second host computers are among the predetermined plurality of host computers for which security is required, and if not, proceeding to step 5, and if so, proceeding to step 3;

(3) encrypting the first data packet in the first bridge computer;

(4) in the first bridge computer, generating and appending to the encrypted first data packet an encapsulation header, including:

(a) key management information [identifying] providing a mechanism for identifying the predetermined encryption method, and

(b) a new address header representing the source and destination for the first data packet, hereby generating a modified first data packet;

(5) transmitting the first data packet or the modified first data packet from the first bridge computer via the internetwork to the second computer network;

(6) intercepting the first data packet or the modified first data packet at the second bridge computer;